NISTTech

Enterprise Software

Specifies and enforces arbitrary attribute-based access control policies

Description

This invention is a standards-driven framework called, the Policy Machine, that provides an enterprise-wide role-based access control (RBAC) environment to control complex access to computer networks. This mechanism represents a shift in specifying and enforcing policy, but more importantly provides a novel and effective way to develop and provide application services in a comprehensive, flexible manner. This technology offers an all-inclusive enterprise-wide software solution that encapsulates the operating system and business applications within a high-confidence environment.

It is a general attribute-based access control method that selects an attribute-based access control policy for specification and enforcement, establishes a configuration of basic data sets in an access control database for the selected attribute-based access policy, and establishes a configuration of basic relations between the basic data sets to control how the policy is enforced.

Applications

- **Network security**
  Security protocols that can be interwoven with operating systems

Advantages

- **File sharing protection**
  Robust security of enterprise applications as files are shared within role-based architecture

Abstract

Protection of enterprise resources in today's access control paradigm requires the deployment of a multitude of access control mechanisms implemented at both the operating system and application levels. These mechanisms come in a wide variety of forms each with their individual methods for authenticating users, configuring security policies, computing access control decisions, and enforcing these policies. A characteristic of dispersed heterogeneous access control mechanisms is a lack of interoperability that consequently results in a host of identity and privilege management issues. However, solving the interoperability problem alone is not sufficient in curing the problems of the existing access control paradigm. While

there exists a diverse set of known access control policies, only a small subset of these policies is enforceable through existing mechanisms. In addition, policies independently implemented within applications can easily undermine one another as well as those implemented at the operating system level. To streamline identity and privilege management operations and provide comprehensive and flexible security policy enforcement, National Institute of Standards & Technology (NIST) has developed a standards-driven framework, called the Policy Machine, for the specification and enforcement of access control that can be adopted by future versions of operating systems and serve as a basis for the development of truly secure applications.

Inventors

- Ferraiolo, David
- Gavrila, Serban I.

Citations

1. J.F. Barkley, A.V. Cincotta, D.F. Ferraiolo, S. Gavrilla, D.R. Kuhn, Role based access control for the world wide web, ACM Transactions on Information and System Security, Vol. 2, No. 1 Feb (1999).
2. D.F. Ferraiolo, R. Chandramouli, G.J. Ahn, S.I. Gavrila. The role control center: features and case studies. Proceedings of the eighth ACM symposium on Access control models and technologies. 2003.
3. R. Sandhu, D.F. Ferraiolo, D, R. Kuhn. The NIST Model for Role Based Access Control: Toward a Unified Standard. Proceedings, 5th ACM Workshop on Role Based Access Control, July 26-27, 2000.
4. DF. Ferraiolo, R Sandhu, S. Gavrila, D.R. Kuhn. R Chandramouli. Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security (TISSEC). Vol 4, issue 3, August 2001.
5. D.F. Ferraiolo, S. Gavrila, V. Hu, R. Kuhn. Composing and Combining Policies under the Policy Machine.Proceedings of the tenth ACM symposium on Access control models and technologies. New York, 2005.

References

- U.S. Patent Application #20090205018
- Docket: 08-015

Status of Availability

This invention is available for licensing.

Last Modified: 12/30/2010